NIST Special Publication 800-9

Good Security Practices for Electronic Commerce, Including Electronic Data Interchange

Roy G. Saltman, Editor

C O M P U T E R S E C U R I T Y

Computer Systems Laboratory

National Institute of Standards
and Technology
Gaithersburg, MD 20899

Sponsored by:
Information Systems Security Officer
Farmers Home Administration
U.S. Department of Agriculture

December 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal Government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 800 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 800-9
Natl. Inst. Stand. Technol. Spec. Publ. 800-9, 66 pages (Dec. 1993)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1993

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402–9325

GOOD SECURITY PRACTICES FOR ELECTRONIC COMMERCE, INCLUDING ELECTRONIC DATA INTERCHANGE

Roy G. Saltman, editor

FOREWORD

This report is an edited version of material submitted to NIST by Robert V. Jacobson of International Security Technology, Inc. of New York City, under contract number 43NANB311675. The contract was sponsored by the Information Systems Security Officer of the Farmers Home Administration, U.S. Department of Agriculture.

ABSTRACT

Electronic commerce (EC) is the use of documents in electronic form, rather than paper, for carrying out functions of business or government that require interchange of information, obligations, or monetary value between organizations. Electronic data interchange (EDI) is the computer-to-computer transmission of strictly formatted messages that represent documents; EDI is an essential component of EC. With EC, human participation in routine transaction processing is limited or non-existent. Transactions are processed and decisions are made more rapidly, leaving much less time to detect and correct errors. This report presents security procedures and techniques (which encompass internal controls and checks) that constitute good practices in the design, development, testing and operation of EC systems. Principles of risk management and definition of parameters for quantitative risk assessments are provided. The content of the trading partner agreement is discussed, and the components of EC, including the network(s) connecting the partners, are described. Some security techniques considered include audit trails, contingency planning, use of acknowledgments, electronic document management, activities of supporting networks, user access controls to systems and networks, and cryptographic techniques for authentication and confidentiality.

Key words: commerce; computer; data; electronic; interchange; internal control; security; techniques.

ACKNOWLEDGMENTS

Assistance of the following persons in the development of material for this report is gratefully acknowledged:

Mr. Michael S. Baum, Esq., President, Independent Monitoring, Cambridge, MA.
Dr. Dennis Branstad, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. Robert P. Campbell, CEO, Advanced Information Management, Woodbridge, VA.
Mr. Hugh V. Davis, Director, Security and Standards Division, U.S. Customs Service, Washington, DC.
Mr. Paul Hoshall, Director, ADP/IRM Audit Division, U.S. Department of Veterans Affairs, Washington, DC.
Mr. David F. Kent, CISA, Director, Office of Information Technology and Financial Audits, U.S. Department of Transportation, Washington, DC.
Mr. F. Lynn McNulty, Associate Director for Computer Security, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. Brent Melson, Information Systems Auditor, Headquarters, National Aeronautics and Space Administration, Washington, DC.
Mr. James Morgan, Manager of Security, GE Information Services, Rockville, MD.
Mr. Paul E. Moo, Electronic Commerce Consulting, Allen, TX.
Mr. Donald Mutispaugh, Defense Logistics Agency, U.S. Department of Defense, Alexandria, VA.
Mr. Edward Roback, National Institute of Standards and Technology, Gaithersburg, MD.
Mr. David Schwarz, Chief, Information Policy Branch, Environmental Protection Administration, Washington, DC.
Ms. Julie A. Smith, CISSP, Research Fellow, Logistics Management Institute, Bethesda, MD.
Mr. John L. Stelzer, Senior EDI Consultant, Sterling Software, Dublin, OH.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

TABLE OF FIGURES

page

1. MANAGEMENT OF SECURITY FOR ELECTRONIC COMMERCE

1.1 New Methods, New Risks

Electronic commerce (EC) is the automated conduct of business processes between and within organizations, using documents and monetary transfers that are in electronic form. EC is carried out using electronic funds transfer (EFT) for monetary interchanges and electronic data interchange (EDI) for non-monetary documents. EDI is the interchange of strictly formatted electronic documents between computers of different organizations. The strict formatting makes possible the use of computer programs to assemble electronic documents from data in computerized applications to begin an interchange and, following receipt of an interchange, to disassemble the documents and insert their data into the receiving organization's computerized applications.

The use of EC introduces new ways of carrying out business operations by eliminating paper-based commerce. The lack of hard-copy records and manual signatures raises the potential for new types of threats to the integrity of operations. Specific activities must be undertaken to assure that electronic documents are authentic, are properly authorized, are completely and accurately retained with audit trails for purposes of accountability, and remain confidential when that is necessary. In addition, operations are heavily dependent on the reliability and availability of electronic devices. It is necessary to detect and recover from error conditions, and to provide effective contingency plans in the case of system failure. It is the role of senior management to assure that the necessary practices and procedures are in place and that these requirements are met.

1.2 Functionality With Security

Senior managers have a vital role in providing for a balanced development program for EC systems that includes adequate provision for security. Authorities agree that this role is essential to successful implementation of EC systems. Senior managers must make sure that there is a proper balance between functionality and security during the design process.

Implementation of an EC system requires more care than a traditional automated business system because of four factors unique to EC:

1) Most traditional paper records are eliminated.

The electronic documents that replace paper documents are extremely important. Care must be taken to safeguard them against loss and alteration, and to ensure that any document can always be retrieved from the secure database in which it has been stored.

2) Human participation in routine transaction processing is limited or non-existent.

Human oversight in paper-based systems has provided formal and informal reasonableness testing and error detection and correction. The EC application programs and the EDI software must include comprehensive controls and checks to replace all aspects of routine human oversight while providing detection of exceptional conditions that trigger special human intervention. This report does not attempt to make a sharp distinction between "security procedures and techniques" and "internal controls and checks." Both security and control objectives are commonly served by the same measures.

3) Transactions are processed more rapidly, leaving less time to detect and correct errors.

Errors must be detected and corrected quickly, before automatic initiation of subsequent actions that will be expensive to correct.

4) Trading partners' computer systems communicate directly with one another.

Each trading partner depends heavily on the accurate and timely performance of the other partners and the data communications network that connects them. EC commonly leads to re-engineering of business systems to take advantage of the speed and efficiency inherent in EC. As a result, each trading partner must be prepared to recover quickly from system failures to avoid having an impact on operations of the other trading partners. Interrupted transactions must not be lost or incorrectly duplicated as a result of retransmission.

As long as nothing goes wrong, an EC system can function without including the security techniques described in this report. However, in the real world, accidents happen, control and procedural failures occur, and people make mistakes. Without an appropriate level of security and control, EC operation will be unreliable, and losses will be unnecessarily high. While EC systems must be protected against fraud and unauthorized disclosure of information, protection against accidents, errors, and omissions is equally important. Because of the increased processing speed of EC transactions, errors can propagate rapidly. As a result, the cost to recover from the consequences of errors and omissions tends to be greater than with traditional business systems. Consequently, prompt, accurate, and automated detection of errors and omissions is an important requirement of EC systems.

In the subsections that follow, seven topics are discussed that senior managers should consider when reviewing the plan to implement an EC system:

1) Initial considerations in planning;

2) Prudent management of the risk factors;

3) Drafting of a trading partner agreement;

4) Testing and commencement of operation;

5) The EC system contingency plan;

6) Management of electronic documents; and

7) Selection of an EDI network.

1.3 Initial Considerations in Planning for EC

An organization typically implements an EC system for one of two reasons:

1) Senior managers, together with application managers and information systems managers, determine that by eliminating traditional paper documents and their routine human processing, an EC system can yield significant savings of time and money. In this case, the organization takes the initiative, and proposes the implementation of an EC system to its trading partner(s). More and more Federal agencies and large business organizations have reached this conclusion.

2) A major customer or agency with which the organization has a business or data-interchange relationship already has an EC system, or plans to implement one. The organization is asked to do likewise. In this case, the organization is being asked either to conform to an existing EC system design or to collaborate in the design of a new EC system.

In the next two subsections, these situations are considered, and the factors that senior managers should consider when planning an EC system implementation are discussed. A senior manager, even if associated with a large organization that is taking the initiative to adopt EC, should also consider the second case. It is useful, to promote smoother implementation in the long run, to be able to see the situation from the point-of-view of the smaller organization and allow for its concerns.

Two trading partners will be assumed. However, in the general case there will be many trading partners, and references to "the trading partners" should be taken to mean all of them. Furthermore, it should be understood that, in some cases, the relationship will not involve trade in goods and services. For example, a government agency may establish an EC system to accept filings from private-sector organizations in response to its regulations. Then the "trade" is in information. For simplicity, the term "trading partners" will be used for all these relationships.

1.3.1 Initiating an EC Development Project

There are two important ingredients in a successful EC system development project: effective cooperation between trading partners in the development of the system specifications, and the adoption of a phased development plan.

When a dominant organization is initiating the development of an EC system, it may assume that it can correctly anticipate the operational needs of the prospective trading partners, and can perform the system design without consulting them. This is probably an unwise assumption, particularly regarding security issues. Many of the security techniques described in this report depend on the effective cooperation of the trading partners. Consequently, it is important to involve prospective trading partners in the development of the basic system design and in the selection of cooperative controls and security techniques and procedures.

Conceptually, the development of an EC system can be thought of as following a three-step sequence:

1) first, substitution of EDI messages for paper documents with continuation of manual processing of the EDI documents;

2) second, automated processing of the EDI messages; and

3) third, re-engineering of applications to take maximum advantage of the speed, accuracy, and standardization offered by EDI.

These steps can be described in more detail as follows:

In the first step, paper documents are translated into EDI formats and delivered electronically to the recipient trading partner. At the most primitive level, the recipient trading partner uses an EDI translation software program to convert incoming EDI messages into traditional formats and to print them. Next, the printed documents are processed as though they had been received in the mail. Similarly, outgoing documents are key-stroked from paper documents into an EDI translation software program and then transmitted to the trading partner. This is obviously a very inefficient practice, but it has the advantage of demonstrating that the "mechanical" part (the EDI part) of an EC trading partnership is functioning correctly. That is to say, the trading partners are able to exchange and translate EDI messages successfully.

In the second step, automated links are established between the existing applications and the organizations' EDI systems. Outgoing messages are generated automatically by the sender's applications, and are no longer key-stroked into the EDI system. Likewise, incoming EDI messages are translated into input files and passed to the recipient's applications automatically. The applications are

enhanced to allow for the monitoring of the EDI interface. For example, the sender's applications are modified to respond to failures of recipients to acknowledge messages on time. The recipient's applications are improved to permit the testing of the reasonableness of incoming messages more rigorously than typical edit checks and to detect duplicate messages.

In the third and final step, applications and business functions are re-engineered to take full advantage of EC. For example, advanced shipping notices sent via EDI could be used to expedite receiving dock and warehouse operations, and to initiate payment without requiring separate generation and processing of an invoice.

When an EC partnership reaches the third step, the partners get the full benefit of EC. The cost of most human processing of paper is eliminated and the attendant errors are avoided, but often there are even greater benefits from more efficient and focused operations. For example, inventories and manufacturing material stocks can be controlled more closely. The time to process orders is reduced. This evolution of existing systems to full-scale EC has repeatedly demonstrated changes that result in functional and quality control improvements. A closer and more efficient relationship is built between the trading partners.

Enthusiastic system designers may want to bypass the first two steps and go directly to a re-engineered EC system. However, converting from paper documents to EDI messages, and substituting automated processing for human oversight, are both big steps. Unexpected problems of the sort described in the remaining chapters of this report can arise. When an organization attempts to go directly from existing paper-based commerce to a phase three, re-engineered EC system, these problems are likely to emerge and cause major losses. Experience suggests that an organization without strong prior experience with EC and EDI should use a phased development. The organization should leave the existing paper-based system in place and use it to deal with the majority of the trading partners while it develops the EC system with a small subset of its trading partners.

The following guidance is proposed for prudent implementation:

1) Begin by picking a single functional area where the application programming is stable and smooth running.

2) Work with a small, but representative, subset of prospective trading partners.

3) Take each of the three development steps described above, one by one. Note that, until all of an organization's major applications have been converted to EC, only limited re-engineering is possible.

When the initial EC system development is complete, consider how to phase-in the remaining trading partners. For example, one might add trading partners in groups over time, and then expand the scope to include other applications.

It is likely that the re-engineering phase will follow paths not originally anticipated, and that the relationship with trading partners will change. These factors suggest that care should be taken to see that the system design allows for growth in size and scope, and changes in operations.

A final note: The organization that initiates an EC system should take care to avoid making unreasonable demands of its subordinate trading partners. While the dominant trading partner may have the resources and expertise to handle an EC system development project easily, this may not always be true of the subordinate partners. The dominant trading partner should take these limitations of resources and expertise into account when planning the role of the subordinate partners.

1.3.2 Joining an Existing EC System

An organization that is being asked to participate in an existing EC system may not have the opportunity to participate in the EC system design. However, the organization will have to decide how to modify its existing operations to accommodate EDI messages. The safest plan is to follow the same three steps described above, using the overall specifications already set by the other trading partner. For example, the organization may begin its participation in an EC system by setting up an EDI system that simply translates EDI messages into paper documents for manual processing. Note however, that the EC system is likely to require acknowledgment of incoming EDI messages. Therefore, it will be necessary initially to establish manual procedures to generate these acknowledgment messages. (See Section 3.2 for more about acknowledgments.)

Next, the EDI system and the applications are enhanced to pass the translated EDI messages to the applications automatically. Applications are enhanced to generate outgoing transactions automatically, including acknowledgments, for processing by the EDI system. Finally, the organization re-engineers its applications to track the operations of the dominant trading partner.

The organization should perform a risk assessment to be sure that all significant risks have been identified and will be properly addressed.

1.4 Risk Management of EC Systems

It is important to manage risk, i.e., the likelihood of loss, as the basis for wise selection of security measures. If all EC

systems were the same: i.e., the same size, transaction volume, information sensitivity, urgency, monetary activity level, and operating environment, it would be possible to define an appropriate security program and apply it to all EC systems without further consideration. This is not the case; EC systems vary in all the dimensions just enumerated. Consequently, it is not possible to define a single security program for all EC systems. EC risks can only be managed efficiently by using rational risk management. Perfect security (nothing will ever go wrong) is infinitely expensive and cannot be a rational design goal. On the other hand, inadequate security often leads to unnecessary losses.

1.4.1 Risk-Sensitive Design

Risk cannot be managed abstractly. The first step in EC system development is to develop a basic system design that accomplishes the functional requirements of the EC system. Security features need not be considered at this point. When the system design is sufficiently detailed, the risk management process can begin. There are three parts to this process:

1) Assessment of risks to determine what kinds and amounts of losses are likely to occur when the EC system becomes operational. Two loss categories are usually identified. (a) Losses caused by threats with reasonably predictable occurrence rates are sometimes referred to as "expected losses," and are expressed as average rates of loss in dollars per year. (b) If a threat has a very low rate of occurrence that is difficult to estimate, but the threat would cause a very high loss if it were to occur, the result would be referred to as a low-probability, high-consequence risk. This type of loss is often called a "single occurrence loss." Chapter Two identifies and describes the risks and vulnerabilities that are associated with typical EC systems.

2) Selection and implementation of security techniques that will (a) reduce expected losses by an amount greater than the cost to implement the security techniques, or (b) reduce the fatal losses to tolerable levels. Chapter Three suggests security techniques for consideration.

3) Periodic re-examination of risks after operational use begins to verify that security techniques continue to be effective, and to detect significant changes in the risk environment.

The initial risk assessment does not have to be highly detailed and precise. Instead, the objective should be to develop a broad understanding of inherent risks and potential security techniques to support the design effort. Thereafter, the first two steps are repeated as necessary during the design phase to refine the assessment; the selection of security techniques is optimized as the EC system design evolves.

The assessment of risks should take into account the effect of the EC technology on the effectiveness of traditional controls. Fewer people do jobs with wider scope. There is reduced routine human oversight. Separation of duties may be diminished, particularly in smaller organizations. These trends may create a situation in which one person can create a false purchase order and acknowledgment for a non-existent vendor, fake a receiving report, and trigger a fraudulent payment through electronic funds transfer.

The third step above is ongoing during the operational life of the EC system to ensure that the security program continues to meet the requirements.

1.4.2 Objectives of a Risk Assessment

Risk management has two basic objectives:

1) Optimization of the selection and implementation of security techniques, based on a rational assessment of risks. "Optimize" in this context means the implementation of security techniques that minimize the sum of future losses and security expenditures. In the case of government agencies, losses could result from compromise of confidentiality or integrity of personal or trade-secret information stored by the agency, as well as direct financial loss of material assets or funds.

2) Protection against catastrophic losses. A catastrophic loss for a private-sector firm would be a loss greater than its equity. In other words, if the loss event occurs, however unlikely its occurrence may be, the loss will bankrupt the firm. While the concept of bankruptcy does not apply in the same way to government agencies, such agencies have a responsibility to the taxpayers to mitigate exposures to material losses.

To meet these two risk management objectives, it is useful to evaluate in monetary terms the risks to which an EDI system is exposed. This enables one to measure the utility of proposed security techniques and to identify potentially catastrophic risks. An assessment of risks in monetary terms uses three kinds of input data:

1) The rate of occurrence of the threats to the EC system.

2) The loss potential associated with each of the functions performed by the EC system and each of the assets controlled by the EC system. Loss potential is the worst-case loss of an asset or function.

3) The vulnerability of the functions performed and organizational assets to each of the threats. Vulnerability is expressed as a "vulnerability factor," which is the ratio of actual loss to loss potential, and ranges from zero to one. Note that a vulnerability by itself is not significant. Even though an asset may be

vulnerable to a threat, the vulnerability is not significant unless the threat is expected to occur. Thus, a vulnerability assessment may yield useful insights about the state of existing security, but it is NOT a risk assessment.

In the real world, the details of threats, vulnerabilities, functions performed, and assets can be quite complex. Consequently, a key part of the risk assessment process is the construction of a model of the EC system that aggregates these elements into manageable groups. Initially, a model can be fairly simple. Then, as the assessment identifies the critical threats, functions, and assets, more detail can be added. This approach ensures that the analysis effort is concentrated on the key issues.

1.4.3 Quantitative Risk Assessments (QRAs)

The cost of security techniques is measured in monetary terms. Therefore, one must also measure the benefit of security techniques (the expected reduction in future losses) in monetary terms to compare cost and benefit. This is the basic reason for performing a QRA. Installing a security technique is not prudent unless its benefit outweighs its cost. The benefit of a security technique is the effect it will have on future losses. A QRA generates an estimate of the monetary losses that will occur in the future based on quantitative estimates of the threat occurrence rates, asset and function loss potentials, and vulnerabilities defined by the model of the system. QRAs are expressed in two ways:

1) Annualized Loss Expectancy (ALE). ALE is the estimated loss expressed in monetary terms at an annual rate, for example, dollars per year. The ALE for a given threat with respect to a given function or asset is equal to the product of the estimates of occurrence rate, loss potential, and vulnerability factor. If the threat's occurrence rate is less than once per year, the ALE must be understood to represent the relative significance of a threat compared with other threats. For example, imagine that the occurrence rate of a threat is estimated to be once in ten years, and its ALE is estimated to be $1,000 per year. This does not mean that the threat will cause a $1,000 loss in each of the next 10 years; it is likely to cause a $10,000 loss in one of the next 10 years, but the specific year of occurrence cannot be determined.

However, if one estimates ALEs for two threats as $1,000 per year and $100,000 per year respectively, all other things being equal, the second threat is clearly far more significant than the first one. Thus, ALE is a useful tool for ranking risks, even though confidence in ALE estimates tends to decrease as occurrence rate decreases. In other words, it is difficult to make credible estimates of occurrence rate for relative rare threats. Nonetheless, even when quantitative estimates are relatively uncertain, they may, in some cases, provide more risk management guidance than purely qualitative estimates of risk.

2) Single-Occurrence Loss (SOL). SOL is the loss expected to result from a single occurrence of a threat. It is determined for a given threat by first calculating the product of the loss potential and vulnerability factor for each function and asset with respect to the threat being analyzed. Then, the products are summed to generate the SOL for the threat. Since the SOL does not depend on an estimate of the threat's occurrence rate, it is particularly useful for evaluating rare but damaging threats. If a threat's SOL estimate is unacceptably high, it is prudent risk management to take security actions to reduce the SOL to an acceptable level.

In short, ALE is useful for addressing relatively frequent threats, and SOL is used to evaluate rare threats.

QRAs are used in three ways:

1) For selection of cost-effective security techniques. To undertake this selection, a "baseline" EC system is defined. A "baseline" EC system has just those features required to function correctly as long as no errors or failures occur. By comparing the ALE of a "baseline" EC system with the ALE of the same EC system assuming the presence of one or more proposed security techniques, one can estimate the payback of the proposed techniques. Obviously, the greater the ratio of the payback (reduction in ALE) to the cost of a security technique, the more valuable it will be.

2) For treatment of high SOLs. The SOL estimate of a threat can be used to identify the potentially fatal threats as mentioned above. While the SOL estimate cannot be used to cost-justify security measures, one can determine what needs to be done to reduce the SOL to an acceptable level. Management judgment is required to make the most effective decisions.

3) To prioritize functions and assets. An ALE can be used to prioritize functions and assets relative to one another, and to rank threats relative to one another. This information is useful when making plans for asset protection, disaster recovery, and business resumption planning.

1.4.4 Conduct of a QRA

The preceding sections have provided the basis for carrying out a QRA, but have not been highly explicit in how it might be done. Other sections of this report present additional information that may assist in this regard. For example, Section 2.3 identifies seven specific basic objectives for the security of EDI transaction sets. In the conduct of a QRA, an analyst may wish to review each of these objectives in light of the activities of the system under study, and specify the losses that would occur if the system failed in achieving any of them.

Losses may be more difficult to quantify for some security objectives than for others. For example, failure to receive goods that have been paid for (possibly due to a failure in sender authentication) may generate a clearly quantifiable loss. Even if the goods are received later, correcting the situation that caused the initial difficulty may generate an extra cost. However, loss due to compromise of confidentiality could be less clear if the organization is a government agency and the disclosure concerned personal data relating to members of the general public. The loss to the organization, which determines the selection of security measures, is distinct from the loss to the individuals. The quantitative loss to the latter could be changes in the individuals' ability to obtain future employment or advantageous business relationships. The loss to the organization might be costs of disruptive investigations, a required re-alignment of security plans and personnel, and costs compensating for the difficulty in collecting similar data in the future due to loss of confidence by the public.

1.5 The Trading Partner Agreement

When system integrators link elements of a data processing system, they speak of the "interfaces" between the system elements, and the need for each element to conform with the applicable interface specification. In a traditional business relationship between two organizations, there is no "interface specification" as such. Instead, humans interpret incoming documents, purchase orders, requests for quotations, and the like, and "translate" them as necessary to conform to internal standards. If disputes arise, they are settled based on agreements between the parties and applicable law and regulation, such as the Uniform Commercial Code, or if one of the parties is a Federal Government agency, Federal procurement regulations. These laws and regulations form an implicit "interface specification."

An essential feature of EC is the reduction or elimination of human participation in the routine processing of transactions, and the substitution of automated processing. As a result, it is essential to define precisely the details of all EC transactions. For example, the part of an EC system that composes an EDI message must use exactly the same message format as the part of the other partner's EC system that receives the message. This means that the trading partners must agree on the standards to be used and the specific details of the implementation.

Trading partner agreements (TPAs) are an important part of EC systems. They serve as the "interface specification" between trading partners and provide specific details of the legal agreements that define how the electronic commerce is to be conducted. Qualified legal advice is required when a TPA is drafted. However, the TPA must be more than a legal agreement between two organizations that interchange data. Since the TPA defines how the automated systems

will replace human inspection and interpretation of individual transactions, it must be complete and precise. The subsections that follow discuss the functions of the TPA in more detail.

1.5.1 Defining X12 Transaction Sets and EDIFACT Messages

The TPA must specify the specific transactions that the EC system is going to process, and the responsibilities of each of the partners for processing transactions. The turn-around time for responding to each EDI message should be specified. The TPA might define how frequently trading partners are required to download messages from network mailboxes. Finally, the TPA must specify what constitutes "receipt" and "acceptance" of a message by the recipient.

Of course, the TPA must include a complete and detailed specification for the format of the EDI message associated with each transaction. Currently, TPAs written in the United States commonly define message formats by reference to the EDI standards adopted by Accredited Standards Committee (ASC) X12. The X12 Committee was chartered in 1979 by the American National Standards Institute (ANSI). FIPS PUB 161-1, Electronic Data Interchange, published by the National Institute of Standards and Technology (NIST) in 1991 and updated in 1993, "adopts, with specific conditions, the families of standards known as X12 and EDIFACT," and requires the use of X12 transaction sets or EDIFACT messages if they meet "the data requirements" of an agency implementing an EC system.

The X12 Committee uses the term "transaction set" to apply to a message devised under its original syntax, data segment directory, and data element dictionary. However, the X12 Committee has voted to adopt the EDIFACT syntax by 1997. EDIFACT, an acronym for Electronic Data Interchange For Administration, Commerce, and Transport, is a family of international standards developed by the United Nations Economic Commission for Europe- Working Party (Four) on Facilitation of International Trade Procedures (UN/ECE/WP.4). The EDIFACT standards define "messages" that can be designed to be functionally equivalent to X12 transaction sets.

It may be convenient to include transaction set information in an Appendix to the TPA, and to include X12 or EDIFACT standards by reference. Note that, in general, versions and releases of these standards are not necessarily upward or downward compatible. If an existing transaction set standard does not exist, the trading partners should conform to the basic conventions used by the X12 Committee when developing their own transaction sets. FIPS PUB 161-1 states that agencies "should use current X12 and/or EDIFACT standards to the extent possible" when working with subject matter not yet considered for EDI standardization, and "shall explicitly submit their requirements for X12 and EDIFACT standards" when EDI standards do not meet agency requirements.

1.5.2 Avoiding and Resolving Disputes

Since system failures, errors, and omissions are going to occur, the TPA should attempt to anticipate each of them, and assign responsibility for their resolution. One approach to drafting the TPA is to consider the operation of the proposed EC system, and to construct a list of all the possible disputes that might arise. The results of the risk analysis will be of help here. Then, the methods of resolution of each dispute should be considered. In the best case, it will be possible to set forth in advance a sequence of steps that will lead to dispute resolution. This analysis may also suggest ways to revise or enhance the EC system controls and security measures to reduce the likelihood that a given dispute will arise, or that it cannot be resolved easily.

Coordination between the trading partners is important for success. For example, acknowledgment of messages is an important control and security technique, and is discussed in Chapter Three. However, it is essential that the trading partners agree on the details of the acknowledgment. Inadequate coordination may result in unrecognized differences in interpretation of such items as operating modes, meanings of transaction sets or messages, responsibility for exception detection, and terms of sale.

As a rule, detection of errors and omissions is much less costly than prevention. For example, recipient acknowledgment of a message can include validation information so that message alterations can be detected easily. The sender's application that processes the acknowledgment can use the validation information in the acknowledgment to verify that transaction sets were received unmodified. This kind of control is relatively simple to implement, but careful coordination between the trading partners is required to make it effective.

1.5.3 Contingency Plans and Disaster Recovery

Recovery from service interruptions, loss of data files, and destruction of system elements is another area where close coordination is required. The flow of transactions can be interrupted by a failure of any one of the five EC system elements defined in Section 2.5. The trading partners must agree on how to handle the interruptions since the actions taken will depend on which element has failed, and the estimated time required to restore service.

Each trading partner must be assured that the other partner can meet agreed-to timeliness goals. A requirement for regular disaster recovery testing should be a part of the TPA for this reason.

1.5.4 Protection of Confidential Data

One objective of the EC system risk analysis should be to identify proprietary, personal, confidential, or classified information that

must be protected against unauthorized disclosure. These data should be identified in the TPA, and the obligations of the partners to protect the data should be defined. Finally, the TPA should specify how long each copy of proprietary, personal, confidential and classified data are to be retained. See Section 1.9 for more about data retention.

1.5.5 Message Authentication and Digital Signatures

Depending on the character of the commerce being conducted, message authentication and digital signatures may be desirable or required by law or regulation. Message authentication is the process whereby the recipient of a transaction set can determine that the transaction set has not been modified during transmission. Digital signatures are elements added to a transaction set or message that are typically used as the equivalent of written signatures on paper documents. Digital signatures enable recipients to authenticate the identity of the individual originators of transaction sets. If these features are required, the TPA must identify which transaction sets are to have the features, how the features are to be implemented, and how failures to authenticate transaction sets and signatures are to be resolved. This topic is discussed in more detail in Sections 3.3.5 and 3.3.6.

1.5.6 A Model TPA

A model TPA has been developed by the American Bar Association, and it can be useful in the initial stage of preparing an agreement. The model agreement stresses the contractual issues; it could serve as a useful point of departure for the drafting of an applicable TPA. For a Federal agency, the model TPA should be considered in connection with the requirements of Federal Acquisition Regulations.

1.6 The EC System Test Plan

Experience shows that careful and complete testing is essential to successful implementation of EC systems.

Case Study: A sender's EDI system was designed to use the output it received from an application each day to overwrite a permanent file that served as input to the EDI translation program. The EDI system was never tested for the case when the output from the application was of zero size. Later, during operational use, it was discovered that when the output was zero, the permanent file was not overwritten. As a result, the prior day's transactions were processed again, resulting in the dispatch of duplicate transaction sets. It was necessary for the recipient to "undo" the duplicate sets manually.

Examples like this underscore the point that EC system failures are

particularly troublesome because they usually involve the other trading partner. Recovery and corrective actions are more difficult when more than one organization is involved. It is essential to verify that all interfaces will work correctly regardless of input errors and omissions.

The following are suggestions for the construction of a test plan:

1) Begin by testing the interface between the applications and the EDI system. Test all transactions at all boundary conditions, and verify correct translation. Simulate all possible error conditions and verify correct response of the applications and the EDI system.

2) Simulate trading partner input from the network to the EDI system; verify correct translation and delivery to the recipient applications.

3) When all sender and recipient processing have been completely tested, conduct tests to simulate EDI traffic in both directions at the planned activity levels. Verify correct handling of potential overload conditions such as month-end, quarter-end, and year-end, when traffic levels may be high and timeliness is critical.

4) When both trading partners have completed the above tests in-house, test the EC system operation between trading partners using test transactions and the network. Note: it is essential to be able to generate test transaction sets during initial acceptance testing, and later when adding enhancements to the EC system. The recipient of test transaction sets should always be able to distinguish them from live transaction sets.

5) Using test messages, simulate emergency conditions to verify that the contingency recovery plan works as expected and that trading partners understand their roles. For example, simulate network or EDI system failures that occur during processing of a stream of transaction sets to verify that interrupted transaction sets can be identified and recovered. (Connections could be unplugged or switches temporarily reset to undertake such a simulation.)

Independent testers should design the tests based on the system specifications, with the goal of demonstrating that the system works as intended regardless of input errors, system errors, and breakdowns. The designers of an EC system should not design, conduct, or evaluate the tests of the system because they will have a natural tendency to prove that the system works as designed using normal inputs and under normal conditions. Test planning is also discussed in Section 3.11.